THE SURVEILLANCE STATE

A COMPLETE PUBLIC RECORD: WHAT YOUR GOVERNMENT DID WITHOUT YOUR KNOWLEDGE OR CONSENT

Eight Decades of Confirmed Mass Surveillance, Offensive Malware, Mind Control Experiments, and Evidence Laundering — Verified by Congressional Investigations, Declassified Documents, Court Rulings, and Authenticated Leaks

Compiled April 2026 | Researched Under Independent Veritas Protocol

NOTE

Every program in this document is confirmed by primary government sources: Church Committee Final Reports (1975-76), Rockefeller Commission (1975), NSA Inspector General Reports, FOIA-released documents, authenticated Snowden disclosures, WikiLeaks Vault 7 (confirmed by CIA internal audit), Reuters investigations confirmed by DEA officials on the record, Der Spiegel ANT catalog confirmed by multiple corporate responses and security research, and direct congressional testimony. Nothing in this document is speculation, conspiracy theory, or unverified allegation.

INTRODUCTION: WHAT THIS DOCUMENT IS AND WHY IT MATTERS

You are reading a complete, plain-language account of what the United States government — and the agencies that serve it — confirmed they did to their own citizens over the past eight decades. This is not a political document. It takes no side. It draws no partisan conclusions. It simply assembles, in one place, what the public record says.

Most of these programs were kept secret for years or decades. Most were exposed not because governments chose transparency, but because a small number of individuals — whistleblowers, journalists, congressional investigators, and private citizens who broke into FBI offices — forced them into daylight. Most were defended as legal and necessary when exposed. Most were found by courts or congressional committees to have been neither.

The global population has a right to know this history. Not to foster anger, but to foster understanding. You cannot make informed decisions about privacy, technology, voting, or civil liberties without knowing what governments have already done — and what they are structurally capable of doing — with the tools and legal frameworks that remain in place today.

Who this is written for: Ordinary people. No legal training required. No technical background needed. Every term is explained. Every program is described in plain English. Every claim is sourced so you can verify it yourself.

THE PATTERN THAT HAS REPEATED FOR EIGHTY YEARS

Before reading any specific program, understand the cycle that has repeated without exception since 1945:

- A secret surveillance or intelligence program is created and justified internally as essential to national security.
- The program collects far more information on ordinary citizens than its stated mandate permits.
- Years or decades later, a whistleblower, journalist, or congressional investigator exposes it.
- The agency defends it as legal and necessary. Courts or Congress partially disagree.
- The program is formally ended — and quietly continued under a new name with fewer restrictions.
- The legal reforms written in response to the exposure become the new baseline from which the next generation of programs departs.

SHAMROCK (1945) became Room 641A and PRISM (2007). Total Information Awareness (2002) became XKeyscore (2008). COINTELPRO methods reappeared in documented 2017 FBI surveillance of Black Lives Matter. The tools evolve. The pattern does not. Every reform was reactive. Every new generation of technology outpaced every legal protection designed to contain it.

ERA ONE: THE FOUNDATION — 1945 TO 1975

After World War II, the United States built a surveillance architecture that operated in total secrecy for thirty years. These programs were exposed only because a group of private citizens called the Citizens' Commission to Investigate the FBI broke into a Bureau field office in Media, Pennsylvania in 1971 and mailed classified documents to newspapers — and because a Senate select committee, chaired by Senator Frank Church of Idaho, spent 1975 and 1976 auditing the intelligence community for the first time. What they found shocked the nation.

PROJECT SHAMROCK & PROJECT MINARET
NSA / Army Signal Security Agency | 1945–1975 | 30 years | CONFIRMED: Church Committee

SOURCE: PUBLIC RECORD

What It Was — In Plain English

Starting in August 1945, as World War II ended, the United States government secretly approached the three largest telegraph companies in America — Western Union, RCA, and ITT World Communications — and asked them to hand over every international telegram sent into or out of the United States, every single day, without a warrant, without a court order, and without the knowledge of the senders or recipients.

The companies were initially reluctant. They believed it was illegal. The government assured them they would not be prosecuted. Secretary of Defense James Forrestal personally told company executives in December 1947 that President Truman had authorized the program — but warned that he could not bind future administrations. The companies complied for thirty years.

What Was Actually Collected

Every international telegram. Not suspected terrorists. Not foreign spies. Every telegram. At its peak, 150,000 messages were printed and analyzed by NSA personnel every single month. The collected data was shared with the FBI, CIA, Secret Service, the drug enforcement bureau, and the Department of Defense. No court ever authorized this. No warrant was ever obtained.

Project MINARET ran alongside SHAMROCK and focused specifically on Americans. By 1974 the NSA had compiled a watchlist — nicknamed the Rhyming Dictionary — that contained millions of names, including thousands of U.S. citizens. The list included prominent Americans such as actors Gregory Peck and Joanne Woodward, journalists, politicians, and civil rights leaders — people placed under surveillance for their political views, not for any criminal activity.

How It Was Exposed

Congressional investigator Britt Snider tracked down retired NSA Deputy Director Louis Tordella in September 1975 and interviewed him at his home in suburban Maryland. Tordella confirmed the program. Senate Intelligence Committee Chairman Frank Church subsequently described SHAMROCK as 'probably the largest governmental interception program affecting Americans ever undertaken.' NSA Director Lew Allen terminated it by handwritten memo in May 1975.

VERDICT

Thirty years. No warrants. No court oversight. 150,000 messages per month. Distributed to six agencies. Confirmed by Senate investigation. Source: Church Committee Final Report, Volume III, 1976.

PROJECT MKUltra & OPERATION MIDNIGHT CLIMAX
CIA | 1953–1973 | 20 years | CONFIRMED: Church Committee, Rockefeller Commission, Senate 1977

SOURCE: PUBLIC RECORD

What It Was — In Plain English

In 1953, CIA Director Allen Dulles approved a top-secret program called MKUltra. Its goal was to develop techniques for controlling the human mind — methods for brainwashing, interrogation, and psychological manipulation. The program was

approved at the highest levels of the CIA and ran for twenty years across at least 149 separate sub-projects involving approximately 80 institutions, including universities, hospitals, prisons, and military installations.

The program experimented with LSD, mescaline, MDMA (ecstasy), heroin, barbiturates, methamphetamine, psilocybin, electroshock therapy, hypnosis, sensory deprivation, psychological torture, and radiation — often on subjects who had no idea they were being experimented on.

Who Was Experimented On

Prisoners, who were offered reduced sentences or recreational time in exchange for participation. Patients in mental hospitals who were told nothing. Students at universities including Columbia and Stanford. U.S. Army soldiers who were never informed. And in some of the most disturbing documented cases, members of the public who were lured under false pretenses.

Operation Midnight Climax was a sub-project in which the CIA set up safe houses in New York and San Francisco, hired sex workers to lure men off the street, secretly dosed them with LSD, and then observed their behavior through two-way mirrors while CIA officers drank cocktails and took notes. This is confirmed in Church Committee testimony and declassified CIA records.

The Death of Frank Olson

Frank Olson was an Army scientist working on biological weapons research. In 1953, CIA colleagues secretly added LSD to his drink without his knowledge. Nine days later, he died after falling from the tenth floor of a New York hotel. For decades the government described it as a suicide. His family maintained it was murder. In 1994, his body was exhumed and a forensic examination found evidence inconsistent with a fall — including a blow to the head that appeared to precede the fall. No charges were ever filed. The U.S. government paid his family $750,000 in 1976.

The Cover-Up

In 1973, CIA Director Richard Helms ordered all MKUltra files destroyed. Boxes of documents were shredded. The program survived historical investigation only because approximately 20,000 financial records had been incorrectly filed in a different building and survived the purge. Without that filing error, MKUltra might have remained completely invisible.

V *Twenty years. 149 sub-projects. 80+ institutions. Unwitting American*

VERDICT

civilians used as test subjects. At least one confirmed death. Records deliberately destroyed. Confirmed by Senate investigation 1977. Source: Senate Select Committee on Intelligence, 1977 Hearings; Church Committee Report Book I, pp. 385-422; Rockefeller Commission Report 1975.

COINTELPRO — COUNTER INTELLIGENCE PROGRAM

FBI | 1956–1971 | 15 years | CONFIRMED: Church Committee, Declassified FBI records

SOURCE: PUBLIC RECORD

What It Was — In Plain English

COINTELPRO was not surveillance. It was sabotage. The FBI, under Director J. Edgar Hoover, ran a secret program whose stated purpose was to 'expose, disrupt, misdirect, discredit, or otherwise neutralize' American political organizations the Bureau considered dangerous. Its targets were not foreign spies. They were American citizens exercising their constitutional rights to speak, assemble, and organize.

Who Was Targeted

The program targeted virtually every major social and political movement of the era: the Civil Rights Movement, the Southern Christian Leadership Conference, the Student Nonviolent Coordinating Committee, the NAACP, Martin Luther King Jr., Malcolm X, the Black Panther Party, the Communist Party USA, the Socialist Workers Party, anti-Vietnam War organizations, the American Indian Movement, feminist organizations, environmentalist groups, and the Puerto Rican independence movement.

What the FBI Actually Did

The tactics went far beyond surveillance. The FBI sent anonymous letters designed to create distrust and conflict between leaders of targeted organizations. It planted false stories in newspapers. It used forged documents to incite violence between rival groups. It provided information to local police that enabled raids on activists' homes — including a December 1969 raid on Black Panther leader Fred Hampton's Chicago apartment that ended with Hampton shot dead in his bed while he slept.

In 1964 — just before Martin Luther King Jr. was to receive the Nobel Peace Prize — the FBI sent him a package containing recordings of his private life and a letter that read, in part, as a threat encouraging him to commit suicide before the prize

ceremony. This letter is in the public record. It was confirmed by the Church Committee. The FBI sent it.

It Did Not End in 1971

COINTELPRO was formally halted in 1971 after its exposure. But internal FBI documents dating as late as 2017, obtained through FOIA requests and reported by The Intercept, showed the FBI surveilling Black Lives Matter activists using methods and categories that directly echoed COINTELPRO. The label changed. The practice continued.

VERDICT

Fifteen years of illegal sabotage of American political life. Confirmed assassination facilitation. A death threat sent to Martin Luther King Jr. on FBI letterhead. Confirmed by Church Committee. The Senate report concluded: 'The Bureau conducted a sophisticated vigilante operation aimed squarely at preventing the exercise of First Amendment rights.' Source: Church Committee Final Report, Books II and III, 1976.

OPERATION CHAOS (MH/CHAOS)

CIA | 1967–1974 | 7 years | CONFIRMED: Rockefeller Commission, Church Committee

SOURCE: PUBLIC RECORD

What It Was — In Plain English

Operation CHAOS was the CIA's version of COINTELPRO — except the CIA was legally prohibited from operating domestically. Its charter expressly forbade it from conducting surveillance on American citizens. It did so anyway for seven years. The stated justification was investigating whether foreign governments were funding or directing American anti-war and civil rights movements. The CIA's own internal assessments, reviewed by the Church Committee, consistently found no evidence of significant foreign influence. The surveillance continued regardless.

What Was Collected

The CIA built files on approximately 7,200 American individuals and scrutinized more than 1,000 domestic organizations. Methods included physical surveillance, electronic monitoring, infiltration of activist groups, warrantless mail opening, and coordination with the FBI to share collected intelligence. The CIA specifically targeted anti-war leaders including Dr. Benjamin Spock, Jane Fonda, and Tom Hayden — American citizens engaged in lawful political activity.

VERDICT

Seven years of illegal domestic CIA surveillance. No evidence of the foreign influence it claimed to be investigating. Confirmed by Rockefeller Commission and Church Committee. Source: Rockefeller Commission Report 1975; Church Committee Report Book III, 1976.

ERA TWO: THE INTERNET AGE — 1995 TO 2007

The rise of the internet created surveillance possibilities that previous generations of intelligence planners could not have imagined. The same digital infrastructure that connected the world also created the possibility of monitoring it — not selectively, but comprehensively. The programs built during this era were not designed to watch specific suspects. They were designed to watch everyone, and sort through the data afterward.

CARNIVORE / DCS1000
FBI | 1997–2005 | CONFIRMED: FOIA releases, Congressional testimony

SOURCE: PUBLIC RECORD

What It Was — In Plain English

Carnivore was a piece of software the FBI installed directly at internet service providers — the companies that provide internet access to ordinary Americans. Once installed, it could monitor all internet traffic flowing through that provider: every email sent, every website visited, every file downloaded — by every customer of that provider, not just the specific target named in any court order.

The FBI claimed Carnivore could be precisely targeted to collect only what a court had authorized. Critics — including an independent technical review commissioned by the FBI itself — found that the software had the ability to collect everything and that distinguishing what had been actually collected from what was discarded was impossible from the outside. The FBI eventually replaced Carnivore with commercially available software that performed the same function but was less visible.

VERDI

FBI surveillance software installed inside American internet providers. Capable of monitoring all traffic from all customers. Replaced by commercial successors still in use. Source: FBI FOIA releases; EPIC litigation documents;

C T	*Britannica.*

MAGIC LANTERN & CIPAV

FBI | 2001 onward | CONFIRMED: FOIA, court documents

SOURCE: PUBLIC RECORD

What It Was — In Plain English

Magic Lantern was the FBI's keystroke logger — software covertly installed on a target's computer that records every key they press, capturing passwords, private messages, and everything else they type. CIPAV (Computer and Internet Protocol Address Verifier) was a companion tool that, once installed, sent the FBI a full inventory of the target computer: its unique identifier, every open port, all installed software, the login name, and the last website visited.

Both tools were deployed through the internet — sent as attachments or exploiting software vulnerabilities — and could be installed without the target's knowledge or any physical access to the device.

VERDICT	*Confirmed through court documents and FOIA releases. Both tools remain in the FBI's operational arsenal. Source: FOIA releases; Wired investigative reporting; court filings.*

TOTAL INFORMATION AWARENESS (TIA)

DARPA | 2002–2003 officially; continued covertly | CONFIRMED: Congressional record, NYT 2012

SOURCE: PUBLIC RECORD

What It Was — In Plain English

Total Information Awareness was the most ambitious domestic surveillance program ever officially proposed in American history. Put simply: the government wanted to build a database of everything about everyone. Not suspected criminals. Everyone.

What It Planned to Collect

The official program documents, which are part of the public congressional record, listed the intended data sources: every credit card purchase, magazine subscription, web browsing history, phone call record, academic grade, bank deposit, gambling history, passport application, airline ticket, train ticket, driver's license, gun license, highway toll payment, judicial record, and divorce record of every American. The program also planned to collect medical data including drug prescriptions, fingerprints, facial images, gait analysis, iris scans, and DNA.

The program was headed by Rear Admiral John Poindexter — the same official convicted of lying to Congress during the Iran-Contra scandal, whose convictions were later overturned on a technicality. Senator Ron Wyden called it 'the biggest surveillance program in the history of the United States.'

What Actually Happened When Congress Cancelled It

Congress defunded TIA in 2003 after the public outcry. But a classified annex to the Defense appropriations bill directed that the underlying technology be transferred to other agencies. By 2006, reports confirmed that components of TIA were operating inside the NSA. A 2012 New York Times report described TIA's legacy as 'quietly thriving' at the agency. The program continued under the code name 'Basketball.' The privacy protections that had been part of the original design were abandoned in the transfer.

VERDICT

Formally cancelled. Secretly continued. Every privacy protection stripped out. The technology built to compile dossiers on all 300 million Americans was transferred to the NSA and kept running. Source: Congressional record; Department of Defense appropriations documents; New York Times, 2012; National Academies Press, 2008.

DCSNet — DIGITAL COLLECTION SYSTEM NETWORK

FBI | Active since 1990s | CONFIRMED: FOIA via EFF

SOURCE: PUBLIC RECORD

What It Was — In Plain English

DCSNet is the FBI's nationwide electronic surveillance network — a system that connects FBI wiretapping stations in field offices and covert locations directly into the

telephone infrastructure of every major American carrier. Once set up, an FBI agent in New York can use DCSNet to establish a wiretap on a cell phone in Sacramento, listen to calls in real time, receive text messages, retrieve voicemails, and track the phone's location — all from a computer interface described by a technical expert as point-and-click surveillance.

The system can simultaneously record calls, create searchable archives, stream audio to translators in remote locations, and route intercepts to mobile surveillance vans. Sprint manages the network's private backbone on the government's behalf. By 2007, DCSNet connected to more than 350 telephone switches operated by carriers across the country.

VERDICT

Active and operational. Not a proposed system. A built, running, nationwide wiretap infrastructure permanently wired into American telecommunications. Source: Wired, 2007; documents obtained by EFF via FOIA; ABC News.

ERA THREE: POST-9/11 — MASS COLLECTION BEGINS — 2001 TO 2013

The September 11, 2001 attacks were used to justify a transformation of American surveillance from targeted investigation to mass collection. The legal architecture was rewritten in secret. The technology was built in secret. When whistleblowers attempted to raise concerns through internal channels, they were raided by the FBI and had their careers destroyed. The full scope of what was built was not known to the public — or to most of Congress — until 2013.

STELLAR WIND — WARRANTLESS MASS SURVEILLANCE

NSA | 2001 onward | CONFIRMED: NSA Inspector General Report 2009; Snowden 2013

SOURCE: PUBLIC RECORD

What It Was — In Plain English

Within weeks of the September 11 attacks, President George W. Bush secretly authorized the NSA to conduct warrantless surveillance on American communications. The program — codenamed Stellar Wind — bypassed the Foreign Intelligence

Surveillance Court, which since 1978 had been the legal mechanism requiring the government to obtain a judicial warrant before monitoring Americans. Bush simply decided, on advice from a small group of lawyers in the Justice Department, that he did not need the court.

NSA technical director William Binney — who retired in October 2001 after thirty years at the agency — described Stellar Wind as recording 320 million telephone calls per day at its outset and included monitoring of domestic email. He called the resulting system 'better than anything the KGB, the Stasi, or the Gestapo ever had.'

The Hospital Confrontation

In March 2004, the Justice Department's own Office of Legal Counsel concluded that a component of Stellar Wind — the email monitoring program — was not legal. Acting Attorney General James Comey refused to reauthorize it. White House officials Alberto Gonzales and Andrew Card then drove to George Washington University Hospital, where Attorney General John Ashcroft was recovering from emergency surgery, to pressure the incapacitated official into overruling his own deputy. Ashcroft refused. This incident — confirmed by congressional testimony from Comey himself — is one of the most documented constitutional confrontations in American history.

VERDICT

Warrantless mass surveillance of American communications authorized by presidential order. Confirmed illegal by the Justice Department's own lawyers. Continued despite internal objections. Exposed by NSA Inspector General report leaked by Edward Snowden. Source: NSA OIG Report ST-09-0002, March 2009; Senate Judiciary Committee testimony of James Comey, 2007.

PRISM — DIRECT ACCESS TO TECH COMPANY SERVERS

NSA | 2007–present | CONFIRMED: Snowden 2013; U.S. Court of Appeals 2020

SOURCE: PUBLIC RECORD

What It Was — In Plain English

PRISM is a program that gave the NSA direct access to data stored on the servers of nine of the largest American technology companies: Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, and Apple. The NSA could collect emails, documents, photographs, chat messages, video calls, file transfers, and social networking data — essentially the entire digital life of anyone who used these services.

The access was obtained through legal orders issued under Section 702 of the FISA Amendments Act, which allowed the government to compel companies to hand over data on foreign targets. The legal problem, confirmed by subsequent court rulings, is that this collection inevitably swept in the communications of American citizens as well — and there was no meaningful mechanism to filter them out.

What the Court Said

In September 2020, the U.S. Court of Appeals for the Ninth Circuit ruled that the NSA's bulk telephone surveillance program — the companion to PRISM — was unlawful. The court specifically noted that the intelligence officials who had publicly defended the program under oath had not been telling the truth. No one was prosecuted. The program continued in modified form.

VERDICT

Confirmed by 41 leaked NSA PowerPoint slides. Ruled unlawful by federal appeals court in 2020. Officials who defended it publicly were found by the court to have made false statements. Still operational under Section 702. Source: The Guardian and Washington Post, June 2013; United States v. Moalin, 9th Circuit, September 2020.

XKEYSCORE — 'SEARCH ENGINE FOR THE INTERNET'

NSA | 2008–present | CONFIRMED: Snowden 2013; PCLOB investigation

SOURCE: PUBLIC RECORD

What It Was — In Plain English

XKeyscore is the NSA's primary analysis tool for internet surveillance. Think of it as a Google search engine — except instead of searching the public web, it searches a database of intercepted global internet traffic including emails, web searches, chat messages, social media activity, browser histories, passwords, and usernames.

Edward Snowden, who used XKeyscore in his work, described it this way in an interview with German public broadcaster NDR: 'You could read anyone's email in the world, anybody you've got an email address for. Any website: you can watch traffic to and from it. Any computer that an individual sits at: you can watch it. Any laptop that you are tracking: you can follow it as it moves from place to place throughout the world. It is a one-stop shop for access to the NSA's information.'

XKeyscore also tracks anyone who uses privacy-protecting tools. NSA documents confirmed the system flags users of the Tor anonymity network and readers of the Linux Journal — a technology magazine — as potential targets for deeper investigation, simply for taking steps to protect their own privacy.

The Gamification of Surveillance

Internal NSA documents revealed that the agency created a gamification system within XKeyscore to encourage analysts to use it more aggressively. Analysts who performed especially well at conducting searches earned 'skilz' points and could 'unlock achievements' — treating mass surveillance as a competitive video game.

VERDICT

Active and operational with no meaningful judicial oversight as of the Privacy and Civil Liberties Oversight Board's 2021 investigation. The Board found that XKeyscore continues to capture Americans' communications 'autonomously' without adequate legal review. Source: Snowden disclosures via The Guardian; NDR interview January 2014; PCLOB statement June 2021.

FASCIA, CO-TRAVELER & MYSTIC — LOCATION AND PHONE RECORDING

NSA | Active | CONFIRMED: Snowden 2013

SOURCE: PUBLIC RECORD

What These Were — In Plain English

FASCIA is an NSA database containing trillions of device-location records collected from cell phones worldwide, including those of American citizens, built by tracking signals emitted by phones as they connect to cell towers.

CO-TRAVELER is a program that analyzed location data from FASCIA to identify unknown associates of surveillance targets — anyone whose phone traveled in proximity to a target phone was automatically flagged for investigation, regardless of whether they had done anything or were suspected of anything.

MYSTIC went further: it was confirmed to record 100 percent of all telephone calls made in at least one country — storing them so analysts could rewind and listen to any call made in the previous thirty days, even if the decision to investigate came after the call was made. The Intercept confirmed MYSTIC had been deployed in the Bahamas and Afghanistan. The targeted countries were redacted from published reports at the request of U.S. officials.

VERDICT

Trillions of location records. Complete call recording capability. Retroactive eavesdropping. All confirmed by Snowden documents. Source: Washington Post, December 2013 (FASCIA); Washington Post, December 2013 (CO-TRAVELER); The Intercept, May 2014 (MYSTIC).

THE NSA UTAH DATA CENTER — BLUFFDALE

NSA | Completed 2014 | Cost: $1.5-3 Billion

SOURCE: PUBLIC RECORD

What It Is — In Plain English

The Utah Data Center is a one-million-square-foot facility built by the NSA at Camp Williams near Bluffdale, Utah, between Salt Lake City and Provo. It is the physical storage brain of the American surveillance apparatus — a warehouse of servers designed to hold and process the data collected by every program described in this document.

The facility uses 65 megawatts of electricity continuously — enough to power 65,000 homes — and requires more than 1.5 million gallons of water per day to keep its servers cool. Its estimated storage capacity is measured in yottabytes — a unit of measurement so large that a yottabyte stored on terabyte drives would require one million data centers, filling the combined area of Delaware and Rhode Island.

NSA whistleblower William Binney, who spent thirty-six years at the agency and co-developed the software predecessor to the surveillance programs now housed here, testified that the facility was built specifically to store the content of American communications — not just metadata — for data mining without warrants. The project was initially called the Massive Data Repository. It was renamed the Mission Data Repository because, according to Edward Snowden, 'Massive Data Repository' sounded too creepy.

VERDICT

A confirmed, operational, $3 billion facility designed to store intercepted communications data at a scale that has no precedent in human history. Source: Wired, March 2012; Utah Data Center Wikipedia (confirmed government specifications); William Binney testimony; Snowden interview.

ROOM 641A & UPSTREAM — THE INTERNET BACKBONE TAP

NSA | Active since at least 2003 | CONFIRMED: AT&T technician testimony; Snowden

SOURCE: PUBLIC RECORD

What It Was — In Plain English

Room 641A is the name of a secret room inside AT&T's internet switching facility on Folsom Street in San Francisco. Confirmed in 2006 by AT&T technician Mark Klein, who provided technical documentation to journalists and lawyers, the room contains NSA equipment that splits the fiber optic cables carrying internet traffic — making a complete copy of everything flowing through one of the major arteries of the American internet and routing it to NSA servers.

Upstream is the umbrella name for all NSA programs that work this way — directly tapping the cables that carry internet traffic, rather than requesting data from companies as PRISM does. Upstream collection is capable of intercepting any internet communication that passes through the United States, which — because of how global internet routing works — includes a significant portion of international communications not sent to or from American citizens.

VERDICT

Confirmed by documented physical evidence — circuit diagrams and technical specifications provided by AT&T technician Mark Klein. Confirmed independently by Snowden documents. Active. Source: Mark Klein sworn declaration in Hepting v. AT&T, 2006; NSA Upstream documentation, Snowden disclosures.

STINGRAY / IMSI CATCHERS — FAKE CELL TOWERS

FBI / Local Law Enforcement | Active since 1995 | CONFIRMED: ACLU FOIA; court rulings

SOURCE: PUBLIC RECORD

What They Are — In Plain English

A Stingray is a device the size of a briefcase that pretends to be a cell phone tower. When turned on, it forces every cell phone within its range to connect to it instead of to the real network. This gives the operator the ability to identify every phone in the area, log the unique identifier of every device, track the location of any phone to

within six feet, and — in some configurations — intercept the calls and texts of targeted devices.

The critical point: a Stingray does not selectively target suspects. When activated, it grabs data from every phone in its range — including the phones of people who have nothing to do with any investigation, who are merely walking down the same street.

How Widely They Are Used — and How They Were Hidden

As of confirmed reporting, Stingrays have been used by federal agencies including the FBI, NSA, DEA, ICE, and Secret Service, and by state and local police departments in at least 23 states. The Baltimore Police Department used Stingrays 4,300 times between 2007 and 2015. Florida police used them more than 200 times between 2010 and 2014 without disclosing this to any court or obtaining any warrant.

The FBI required local police departments that purchased Stingrays to sign non-disclosure agreements — legally binding secrecy contracts — preventing them from disclosing their use to defense lawyers, prosecutors, or courts. Police were instructed to describe Stingray evidence in court documents as coming from a 'confidential source' — concealing the true origin from judges and defendants. This practice was confirmed through ACLU FOIA litigation.

VERDICT

Mass surveillance of all phones in a given area, without warrants, used thousands of times, actively concealed from courts through government-mandated secrecy agreements. Baltimore PD alone used them 4,300 times. Source: ACLU FOIA documents; Georgetown University Law Center analysis; Electronic Frontier Foundation; Stingray use in United States law enforcement, Wikipedia citing ACLU research.

ERA FOUR: THE NSA HARDWARE WEAPONS CACHE — 2001 TO PRESENT

Parallel to the mass surveillance programs, the NSA's Tailored Access Operations (TAO) unit was building something else: an arsenal of cyberweapons and hardware implants capable of compromising virtually any electronic device on the market. This was not defensive security work. These were offensive weapons — tools for breaking into systems, stealing data, and in some cases destroying physical infrastructure. When this arsenal leaked, the consequences fell on ordinary people worldwide.

THE NSA ANT CATALOG — 50+ HARDWARE WEAPONS

NSA Tailored Access Operations | 2008 catalog published; active since at least 2001 | CONFIRMED: Der Spiegel December 2013

SOURCE: PUBLIC RECORD

What It Was — In Plain English

In December 2013, the German magazine Der Spiegel published a 50-page classified NSA document from 2008 — a product catalog listing more than 50 surveillance tools and cyberweapons available for order by NSA analysts. The catalog reads like a shopping list. Each item has a code name, a product description, technical specifications, a diagram, and a price. The items range from free software to $250,000 hardware kits. They were designed to compromise virtually every major category of consumer and enterprise technology.

CODE NAME	TARGET	CAPABILITY	PRICE
DROPOUTJEEP	Apple iPhone	Remote access: files, texts, contacts, voicemail, location, hot mic, camera. 100% success rate per NSA documentation.	Classified
COTTONMOUTH-I	USB cables	Hidden RF transceiver in USB cable wirelessly transmits data from any plugged-in computer to NSA receiver.	$200K / 50 units
RAGEMASTER	VGA monitor cable	Wirelessly transmits everything displayed on a monitor to an NSA receiver nearby — clones the screen remotely.	Classified
JETPLOW	Cisco firewalls	Firmware-level permanent backdoor. Survives reboots and firmware updates. Widely deployed per NSA documentation.	Classified
IRATEMONK	Hard drive firmware	Rootkit embedded in hard drive. Survives disk reformatting, data erasure, and OS reinstallation.	Classified

CODE NAME	TARGET	CAPABILITY	PRICE
DEITYBOUNCE	Dell servers	Backdoor via motherboard BIOS and RAID controller. Survives OS reinstalls.	Classified
NIGHTSTAND	Windows XP PCs	Wirelessly installs exploits from up to 8 miles away via crafted WiFi packets.	Classified
MONKEYCALENDAR	Mobile phones	Transmits the phone's location via hidden text messages.	Classified
FEEDTROUGH	Juniper firewalls	Persistent backdoor that survives firmware upgrades.	Classified
HALLUXWATER	Huawei firewalls	Backdoor hidden in boot ROM — impossible to remove without physical hardware replacement.	Classified
HEADWATER	Huawei routers	Persistent remote code execution capability embedded in router.	Classified
COTTONMOUTH-III	Ethernet+USB plug	Stacked connector that creates a covert wireless bridge into the target network.	$1.25M / 50 units
GINSU	PC firmware	Survives complete OS reinstallation via PCI bus firmware.	Classified

Every company whose products appear in this catalog — Apple, Cisco, Dell, Juniper, Huawei, Seagate, Western Digital, Samsung — denied any collaboration with the NSA. The capability existed regardless. The NSA obtained source code through security audits, by posing as software developers, or through classified agreements. The companies may genuinely not have known.

VERDICT

A confirmed, priced, illustrated catalog of 50+ tools for breaking into every major category of consumer and enterprise hardware. Source: Der Spiegel, December 29, 2013, 'NSA's ANT Division Catalog of Exploits for Nearly Every Major Software/Hardware/Firmware.'

THE EQUATION GROUP — HARD

SOURCE: PUBLIC RECORD

DRIVE FIRMWARE IMPLANTS

NSA Tailored Access Operations | Active since at least 2001 | CONFIRMED: Kaspersky Lab 2015; former NSA officials on record

What It Was — In Plain English

Kaspersky Lab researchers announced in February 2015 that they had discovered malware embedded inside the firmware of hard drives — the lowest-level software that runs a hard disk before the operating system even loads. The malware had been placed inside drives manufactured by Seagate, Western Digital, IBM, Toshiba, Samsung, Hitachi, and Maxtor — together representing the vast majority of hard drives sold worldwide.

Former NSA employees confirmed to Reuters that the agency had developed this capability. The key facts are these: once a hard drive is infected at the firmware level, the infection survives complete reformatting of the drive. It survives erasure. It survives reinstallation of the operating system. There is no standard way to detect it because the firmware cannot be read back by normal tools — only written to. Kaspersky's chief security researcher stated: 'It means we are practically blind and cannot detect hard drives that have been infected by this malware.'

The malware also created hidden storage areas on infected drives — secret compartments invisible to the operating system — where the NSA could store data and later retrieve it. The program had been running for approximately fifteen to twenty years before it was discovered.

VERDICT

Confirmed by Kaspersky Lab technical analysis. Confirmed by former NSA officials speaking to Reuters. Hard drives sold to consumers and businesses worldwide were infected with persistent, undetectable, self-hiding malware. There is no way to know how many of the billions of hard drives sold during this period were affected. Source: Kaspersky Lab 'Equation Group: Questions and Answers,' February 2015; Reuters, February 16, 2015.

STUXNET / OPERATION OLYMPIC GAMES

NSA + CIA + Israeli Unit 8200 | 2006–2010 | CONFIRMED: Multiple senior officials on record; Washington Post; New York Times

SOURCE: PUBLIC RECORD

What It Was — In Plain English

Stuxnet was the world's first known cyberweapon designed to cause physical destruction. It was created jointly by the NSA, the CIA, and Israel's military intelligence unit (Unit 8200), authorized by Presidents George W. Bush and Barack Obama under a secret program called Operation Olympic Games. Its target was Iran's uranium enrichment program at the Natanz nuclear facility.

Stuxnet worked by infiltrating the industrial control systems that operated centrifuges — machines that spin at extreme speeds to enrich uranium. Once inside, it secretly commanded the centrifuges to spin too fast, destroying them, while simultaneously feeding false data to monitoring systems so Iranian engineers believed everything was normal. It destroyed approximately 1,000 centrifuges — roughly 20 percent of Iran's enrichment capacity — before it was discovered.

Why It Matters for Everyone

In 2010, a programming error caused Stuxnet to spread beyond the Natanz facility. An infected engineer connected a work laptop to the internet. Within weeks the worm was replicating globally, infecting computers in 30 countries including the United States. Because Stuxnet was designed to target Siemens industrial control systems — systems used in power plants, water treatment facilities, hospitals, and manufacturing worldwide — any organization using that equipment was now carrying a sophisticated cyberweapon, whether they knew it or not.

Microsoft compared the loss of Stuxnet to the U.S. military having some of its Tomahawk cruise missiles stolen. The NSA had created the first weapon capable of crossing from the digital world into the physical world and causing real industrial destruction — and it lost control of it.

VERDICT

Confirmed by named senior officials including former CIA Director Michael Hayden and former NSA Director Keith Alexander. Confirmed by Washington Post (June 2012) and New York Times (June 2012) citing current and former officials. The weapon was lost and is now in the wild. Source: Washington Post, June 1, 2012; New York Times, June 1, 2012; Operation Olympic Games, Wikipedia.

ETERNALBLUE & WANNACRY — THE WEAPON THAT ESCAPED

NSA | Developed ~2012; leaked 2017 | CONFIRMED: Microsoft; Shadow Brokers; multiple

SOURCE: PUBLIC RECORD

governments

What It Was — In Plain English

EternalBlue is a cyberweapon built by the NSA that exploits a vulnerability in Microsoft Windows. It allows an attacker to gain complete control of any Windows computer connected to a network — without needing a password, without any action by the user. The NSA discovered this vulnerability in Windows and, rather than disclosing it to Microsoft so it could be fixed, kept it secret for years and weaponized it.

How It Escaped and What Happened Next

In April 2017, a mysterious group called the Shadow Brokers — whose identity remains unknown — released EternalBlue and other NSA tools to the public. One month later, on May 12, 2017, a ransomware attack called WannaCry used EternalBlue to infect 230,000 computers in 150 countries within 24 hours.

Hospitals in the United Kingdom's National Health Service were locked out of patient records and had to turn away non-emergency patients. Nissan and Renault manufacturing plants in Europe shut down. FedEx, Deutsche Bahn, Telefonica, the Russian Interior Ministry, and hundreds of universities were hit. Subsequent attacks using EternalBlue — including NotPetya, which caused an estimated $10 billion in global damage — continued for years.

All of this damage flowed directly from the NSA's decision to stockpile this vulnerability rather than disclose it. The NSA had been sitting on a defect in software used by hundreds of millions of people worldwide and had said nothing — because it was useful to them. When they lost control of it, the damage fell on ordinary people.

VERDICT

Confirmed by Microsoft, multiple governments, and the Shadow Brokers' own public release. The NSA built EternalBlue, kept the underlying vulnerability secret from Microsoft for years, lost control of the weapon, and 230,000 computers in 150 countries were then ransomwared in 24 hours as a direct consequence. Source: EternalBlue Wikipedia; Microsoft Security Bulletin MS17-010; WannaCry ransomware attack documentation.

ERA FIVE: CIA VAULT 7 — THE COMPLETE HACKING ARSENAL — 2013 TO 2016

In March 2017, WikiLeaks published 8,761 documents from a classified network inside the CIA's Center for Cyber Intelligence at Langley, Virginia. A CIA internal audit subsequently confirmed that 91 malware tools out of more than 500 in active use in 2016 had been compromised. The documents covered CIA hacking operations from 2013 to 2016 and revealed that the CIA had quietly built its own NSA — a parallel cyber intelligence apparatus with over 5,000 registered hackers that had produced more code than Facebook's entire platform.

CIA VAULT 7 — THE FULL CONFIRMED TOOL LIST

CIA Center for Cyber Intelligence | 2013–2016 | CONFIRMED: CIA internal audit; WikiLeaks release

SOURCE: PUBLIC RECORD

What It Was — In Plain English

The CIA's hacking division had built an arsenal of tools capable of compromising virtually every connected device in the world. The following capabilities were confirmed in the Vault 7 documents:

TOOL / PROGRAM	TARGET	CONFIRMED CAPABILITY
Weeping Angel	Samsung Smart TVs	Transforms TV into a covert microphone that records audio in the room and transmits to CIA even when TV appears to be off.
Marble Framework	All CIA cybertools	Disguises CIA malware to appear as if created by Russia, China, North Korea, Iran, or Arabic-speaking countries, defeating forensic attribution.
iOS Exploits (multiple)	Apple iPhones/iPads	Persistent implants. Disproportionate focus due to iPhone popularity among 'social, political, diplomatic and business elites.'
Android Exploits (multiple)	Android phones	Attacks on Samsung, HTC, Sony. Bypass encryption of WhatsApp, Signal, Telegram by attacking the phone itself before encryption applies.
Hammer Drill	Windows CDs/DVDs	Air gap jumping virus that infects software distributed on CDs and DVDs, jumping to computers not connected to the internet.
Brutal Kangaroo	Air-gapped computers	Infects USB drives to carry malware

TOOL / PROGRAM	TARGET	CONFIRMED CAPABILITY
		into computers physically disconnected from the internet.
Assassin / Medusa	Windows systems	Automated implant control systems. Installs malware automatically at scale across CIA operations.
OutlawCountry	Linux systems	Redirects all outbound network traffic on a Linux computer to CIA-controlled servers.
BothanSpy / Gyrfalcon	SSH credentials	Steals login credentials for secure remote connections on both Windows and Linux. Transmits credentials to CIA.
CouchPotato	Video streams	Remotely collects video from security cameras and streaming systems. Captures still images when motion detected.
Dumbo	Webcams	Suspends webcam processes and corrupts video recordings to conceal CIA physical access operations.
ExpressLane	Partner agencies	Covertly exfiltrates biometric data collected by CIA partner agencies — including the FBI, DHS, and NSA — without their knowledge.
Angelfire	Windows XP/7	Persistent implant framework that loads malware before the operating system — impossible to remove by standard means.
Athena	All Windows versions	Full persistent backdoor covering all Windows versions from XP to 10. Remote beacon, file system control, payload deployment.
Pandemic	Windows networks	Replaces legitimate software with trojanized versions as it travels across a network, infecting remote users.

The Security Failure That Made This Worse

A CIA internal audit, released in 2020 following FOIA litigation by CNN, found that the breach occurred because the CIA's Center for Cyber Intelligence was so focused on building offensive weapons that it had 'woefully lax' security. The audit stated: 'We failed to recognize or act in a coordinated fashion on warning signs that a person or persons with access to CIA classified information posed an unacceptable risk to national security.' The amount of data taken was estimated at up to 34 terabytes — equivalent to 2.2 billion pages of text.

The Marble Framework deserves special attention. The CIA built a tool specifically designed to make its own cyberattacks look like they originated from Russia, China, North Korea, Iran, or Arabic-speaking countries. This means that when forensic investigators anywhere in the world attempt to attribute a cyberattack to a nation, they cannot rule out that the CIA designed the attack to appear to come from somewhere else. Attribution of any cyberattack became — by CIA design — permanently uncertain.

VERDICT

Confirmed by CIA internal audit. 500+ tools, 5,000 hackers, more code than Facebook. The CIA was running its own parallel surveillance apparatus with no public knowledge or meaningful oversight. Source: WikiLeaks Vault 7, March 2017; CIA WikiLeaks Task Force Report, October 2017 (declassified June 2020); CNN, June 2020.

ERA SIX: THE EVIDENCE LAUNDERING SYSTEM — ONGOING

What follows may be the most constitutionally consequential finding in this entire document. Every program described above represents secret surveillance. This section describes something different: a documented, institutionalized system for taking the products of potentially illegal surveillance and converting them into 'legitimate' criminal evidence — while hiding the conversion from judges, prosecutors, and defendants.

PARALLEL CONSTRUCTION — THE DEA/NSA EVIDENCE LAUNDERING SYSTEM

DEA Special Operations Division + NSA + FBI + IRS + CIA + DHS | Active since 1990s | CONFIRMED: Reuters 2013; DEA officials on record

SOURCE: PUBLIC RECORD

What It Is — In Plain English

Parallel construction is a process in which law enforcement agencies receive intelligence tips derived from classified surveillance — including NSA phone intercepts — and then build a second, parallel set of evidence to use in court. The goal is to make it appear that the investigation began through normal, constitutional means, while concealing the true origin of the tip.

How It Works — A Concrete Example

The NSA intercepts a phone call that reveals a specific person will pick up a drug shipment at a specific truck stop at a specific time. Rather than use that intercept as evidence — which would require disclosing the NSA's surveillance to defense lawyers and courts — the DEA's Special Operations Division passes a tip to state troopers: be at that truck stop at that time, look for that vehicle. The troopers wait, stop the car for a minor traffic infraction, run a drug dog, and 'discover' the shipment. The court record shows: routine traffic stop, dog alert, drugs found. The NSA is never mentioned.

This Is Confirmed — Not Alleged

Reuters confirmed this in a 2013 investigation, citing documents reviewed by their reporters and interviews with more than a dozen current and former federal agents who confirmed they had used parallel construction in their careers. A senior DEA official told Reuters on the record: 'Parallel construction is a law enforcement technique we use every day. It's decades old, a bedrock concept.'

One former DEA agent summarized it plainly: 'It's just like laundering money — you work it backwards to make it clean.'

The Special Operations Division that manages these tips was confirmed to have 24 partner agencies, including the NSA, FBI, CIA, IRS, and Department of Homeland Security. The IRS itself was confirmed to have received SOD tips and was directed to build parallel evidence trails to conceal the source — meaning tax prosecutions may have been built on NSA intelligence the defendants never knew existed.

Why This Matters

Every defendant in the United States has a constitutional right to know the evidence against them and to challenge its legality. Parallel construction systematically denies that right. If a case began with an unconstitutional NSA intercept, the defendant cannot challenge that intercept if they are never told it existed. They are convicted on evidence whose true origin has been hidden by their own government — from them, from their lawyers, and often from the judge.

VERDICT

Confirmed on the record by senior DEA officials. Confirmed by 12+ current and former federal agents. Documented in internal DEA training materials. IRS independently confirmed to use the same practice. The number of Americans convicted through this process over the decades of SOD operation is classified and unknown. Source: Reuters, August 5, 2013, 'U.S. Directs

Agents to Cover Up Program Used to Investigate Americans.' IRS manual documentation, Reuters follow-up August 7, 2013. EFF analysis, August 7, 2013.

ERA SEVEN: FOREIGN SPYWARE ACQUIRED FOR AMERICAN USE — 2014 TO PRESENT

Beyond what American agencies built themselves, the U.S. government also acquired, tested, and in some cases purchased the most sophisticated commercial surveillance tools developed by foreign companies — tools that foreign governments have used to spy on journalists, activists, and dissidents worldwide.

FINFISHER / FINSPY
Gamma International (UK/Germany) | Used against American on U.S. soil: CONFIRMED 2014

SOURCE: PUBLIC RECORD

What It Is — In Plain English

FinSpy is commercially produced spyware sold to governments and law enforcement agencies worldwide by a British-German firm. Once installed on a device, it provides complete remote access: all calls, texts, emails, files, contacts, browser history, location tracking, microphone activation, and camera activation — delivered to the purchasing government in real time.

Why It Appears in an American Surveillance Document

In 2014, it was confirmed that the Ethiopian government installed FinSpy on the computer of an American citizen living in the United States. The spyware was delivered through a fake Microsoft Word document attachment. For months, recordings of dozens of Skype calls — private conversations of an American in America — were transmitted to Ethiopian government servers. The victim sued. A federal court ruled in 2017 that the Ethiopian government was protected from civil liability by the Foreign Sovereign Immunities Act. The surveillance of an American on American soil by a foreign government using commercial spyware had no legal consequence.

VERDICT

A foreign government spied on an American citizen inside the United States using commercial malware. Confirmed by court proceedings. The American had no legal recourse. Source: Ars Technica, 2014; EFF legal filing; Kidane v. Ethiopia, U.S. Court of Appeals D.C. Circuit, March 2017.

PEGASUS SPYWARE — FBI ACQUIRED AND TESTED FOR DOMESTIC USE

NSO Group (Israel) | FBI acquired 2019; tested for U.S. phone use | CONFIRMED: New York Times; FBI admission

SOURCE: PUBLIC RECORD

What It Is — In Plain English

Pegasus is a spyware tool developed by the Israeli company NSO Group, marketed to governments as a counterterrorism tool. It is the most capable commercial surveillance software ever publicly documented. Once installed — which can be done without the target clicking anything, through what is called a zero-click exploit — Pegasus provides complete control of the target phone: all messages across every application, all calls, all files, live microphone and camera access, and real-time location. It can even access messages that have already been sent or received in encrypted applications like WhatsApp and Signal, by reading them directly from the phone's memory.

The FBI's Involvement

In June 2019, NSO Group set up a dedicated test facility in New Jersey specifically for the FBI, which had procured NSO's services to evaluate Pegasus for use on American phones. For two years, the FBI tested the tool. After internal deliberations, the FBI decided in 2021 not to deploy it for domestic law enforcement. However, a document obtained by the New York Times showed that the agency had explicitly weighed using Pegasus in domestic criminal cases. Despite the decision not to deploy it, Pegasus equipment remains in FBI possession at the New Jersey facility as of confirmed reporting.

American Government Employees Already Targeted

In December 2021, Apple confirmed the first known case of Pegasus being used against Americans: eleven U.S. State Department employees stationed in Uganda had

their iPhones infected. The identity of the government client that ordered the surveillance remains unknown.

VERDICT

The world's most invasive commercial spyware was acquired by the FBI, tested for use on American phones, and seriously considered for domestic deployment. It was explicitly weighed for use in domestic criminal investigations. Pegasus equipment remains in federal possession. American government employees have already been targeted with it. Source: New York Times, January 28, 2022; Apple statement, December 2021; FBI admission.

ERA EIGHT: THE GLOBAL ARCHITECTURE — ECHELON AND THE FIVE EYES

All of the programs described above operate within a larger international framework that has existed since 1946: a signals intelligence sharing alliance between the United States, the United Kingdom, Canada, Australia, and New Zealand, known collectively as the Five Eyes. This alliance created a mechanism for each country to legally collect data on the citizens of the other four — and share it — effectively circumventing each nation's domestic laws protecting its own citizens from government surveillance.

ECHELON / FROSTING — THE GLOBAL INTERCEPTION NETWORK

NSA + GCHQ + CSE + ASD + GCSB | 1966–present | CONFIRMED: NSA newsletters leaked by Snowden 2015; European Parliament investigation 2001

SOURCE: PUBLIC RECORD

What It Is — In Plain English

ECHELON is the code name for the global signals intelligence collection system operated by the five English-speaking nations of the Five Eyes alliance. It was designed to intercept satellite communications, telephone calls, fax transmissions, internet traffic, and radio signals on a global scale. Two NSA internal newsletters from 2011 and 2012, published by The Intercept in 2015 from the Snowden archive, for the first time confirmed that the NSA used the ECHELON code name — ending decades of official denials.

The European Parliament investigated ECHELON in 2000 and 2001 and concluded that the network's existence was 'no longer in doubt.' The parliament's report confirmed ECHELON was capable of intercepting and inspecting the content of telephone calls, faxes, emails, and internet traffic globally. The investigation also found evidence that ECHELON data had been used for industrial espionage — helping American companies win contracts against European competitors.

The Circumvention Architecture

American law prohibits the NSA from spying on American citizens without a warrant. British law restricts GCHQ from spying on British citizens. The Five Eyes arrangement effectively dissolves these protections: the NSA collects data on British citizens and shares it with GCHQ; GCHQ collects data on American citizens and shares it with the NSA. Neither agency has technically violated its own domestic law. The citizens of all five nations are comprehensively surveilled, and none of their legal protections apply.

Edward Snowden described the Five Eyes as 'a supra-national intelligence organization that does not answer to the known laws of its own countries.' This assessment is in the public record.

VERDICT

A confirmed 80-year global interception network. Acknowledged by all five governments. Found by European Parliament investigation to be real and operational. Used for industrial espionage in addition to intelligence gathering. Creates a legal circumvention mechanism allowing each nation's intelligence agency to spy on that nation's own citizens through its partners. Source: NSA newsletters 2011-2012 published by The Intercept, August 3, 2015; European Parliament Report on ECHELON, 2001; Five Eyes Wikipedia citing government acknowledgments.

THE PEOPLE WHO TRIED TO STOP IT

The public knows about these programs because specific individuals decided that the public's right to know outweighed the personal risks of disclosure. In virtually every case, those individuals were punished — not the programs they exposed.

PERSON	AGENCY / ROLE	WHAT THEY REVEALED AND WHAT HAPPENED
William Binney	NSA Technical Director, 36	Exposed warrantless mass surveillance

PERSON	AGENCY / ROLE	WHAT THEY REVEALED AND WHAT HAPPENED
	years	(Stellar Wind) and the Utah Data Center's true purpose. FBI raided his home at gunpoint. Never charged. His treatment influenced Snowden's decision to go public.
Edward Snowden	NSA contractor	Disclosed PRISM, XKeyscore, MUSCULAR, FASCIA, the ANT catalog, and the full architecture of NSA mass surveillance. Charged under the Espionage Act. Lives in exile in Russia. The NSA program he exposed was ruled unlawful by a federal court in 2020.
Thomas Drake	NSA Senior Executive	Raised concerns about Trailblazer waste and domestic surveillance through internal channels. FBI raided his home. Charged under Espionage Act. Charges later dropped. Career destroyed.
Mark Klein	AT&T Technician	Provided technical documentation confirming Room 641A — the NSA's fiber optic tap inside AT&T. Provided sworn declaration to EFF. Not charged.
Seymour Hersh	Journalist, New York Times	Published 1974 exposé on Operation CHAOS, triggering the Church Committee. Later published reporting on targeted killing programs.
The Citizens' Commission (1971)	Private citizens	Broke into FBI office in Media, Pennsylvania. Stole and published documents proving COINTELPRO. Never identified until 2014 when they came forward voluntarily. Never charged — statute of limitations.
Joshua Schulte	CIA Software Engineer	Source of Vault 7 leak. Convicted July 2022. Sentenced February 2024 to 40 years imprisonment.

COMPLETE MASTER REGISTRY: EVERY CONFIRMED PROGRAM

The following table is the complete confirmed record assembled across three levels of investigation. Every entry is sourced to primary government documents, court rulings, congressional testimony, or authenticated whistleblower disclosures.

PROGRAM	AGENCY	PERIOD	LEGAL STATUS	WHAT IT DID
SHAMROCK	NSA	1945-1975	Illegal. No warrants.	Intercepted every international telegram — 150,000/month at peak. Zero warrants. Shared with 6 agencies.
MINARET	NSA	1967-1973	Illegal	Watchlist of 70,000 Americans including celebrities, journalists, politicians — monitored for political views.
MKUltra	CIA	1953-1973	Illegal. Records destroyed.	Mind control experiments on unwitting civilians, prisoners, students. LSD, electroshock, torture. 149 sub-projects.
Op. Midnight Climax	CIA	1950s-60s	Illegal	Sex workers used to lure civilians to CIA safehouses for secret LSD dosing. Observed through two-way mirrors.
COINTELPRO	FBI	1956-1971	Illegal	Surveillance, infiltration, sabotage, blackmail, and facilitation of violence against American political movements.
Operation CHAOS	CIA	1967-1974	Illegal. Violated CIA charter.	CIA domestic surveillance of 7,200 Americans and 1,000 groups. No foreign influence found. Continued anyway.
HTLINGUAL	CIA	1952-1973	Illegal	Mass opening of Americans' postal mail to/from Soviet Union. No warrants.
Carnivore/ DCS1000	FBI	1997-2005	Replaced	Packet sniffer installed at ISPs. Could monitor all traffic from all customers, not just suspects.
Magic Lantern	FBI	2001-present	Active	Keystroke logger covertly installed on targets' computers. Records everything typed.
CIPAV	FBI	2001-present	Active	Computer ID and activity harvester. Deployed remotely. Full inventory of device and online activity.
Total Info. Awareness	DARPA/ NSA	2002-present	Defunded; continued covertly	Plan to database all Americans' records: purchases, calls, medical, travel, financial. Continued as 'Basketball.'
Stellar Wind	NSA	2001-ongoing	Ruled unlawful	Warrantless collection of American phone calls, emails, internet activity. 320M calls/day at outset.
DCSNet	FBI	1990s-present	Active (CALEA)	Nationwide point-and-click wiretap infrastructure wired into every major American carrier.

PROGRAM	AGENCY	PERIOD	LEGAL STATUS	WHAT IT DID
PRISM	NSA	2007-present	Ruled unlawful 2020	Direct access to data from Microsoft, Google, Apple, Facebook, Yahoo, Skype, YouTube, AOL, PalTalk.
XKeyscore	NSA	2008-present	No judicial oversight	Real-time search of all global internet traffic. Read any email. Watch any website. Track any device.
MUSCULAR	NSA/ GCHQ	Active	Unreviewed	Pure hacking of tech company cables. Twice PRISM's daily data volume. No company cooperation needed.
FASCIA	NSA	Active	Unreviewed	Trillions of device location records. Tracks every cell phone's movement globally.
CO-TRAVELER	NSA	Active	Unreviewed	Identifies unknown associates by proximity of their phone to a target's phone.
MYSTIC	NSA	Active	Unreviewed	Records 100% of all phone calls in targeted countries. Retroactive 30-day playback.
Room 641A/Upstream	NSA	2003-present	Active	Fiber optic tap directly inside AT&T Internet backbone. Copies all internet traffic passing through.
Stingray/IMSI	FBI/Local LE	1995-present	Partially unlawful	Fake cell towers. Grab all phones in range. Used 4,300+ times in Baltimore alone. Concealed from courts.
ANT Catalog (50+ tools)	NSA/TAO	2001-present	Unreviewed	Hardware implants for iPhones, Cisco routers, Dell servers, hard drives, USB cables, monitor cables.
Equation Group/HDD	NSA/TAO	2001-2015+	Unreviewed	Undetectable hard drive firmware malware. Survived reformatting. In drives from all major manufacturers.
Stuxnet/Olympic Games	NSA+CIA +Israel	2006-2010+	Escaped; in the wild	First cyberweapon causing physical destruction. Lost control; now in 30+ countries including the U.S.
EternalBlue	NSA	2017 leaked	Weapon lost	Windows exploit kept secret for years. Stolen and released. Used to ransomware 230,000 computers in 150 countries.
Vault 7 / CIA Arsenal	CIA	2013-2016	34TB stolen	500+ hacking tools. Smart TVs turned to mics. All major phones, OS, browsers compromised. Marble fakes attribution.

PROGRAM	AGENCY	PERIOD	LEGAL STATUS	WHAT IT DID
Parallel Construction	DEA/ NSA/FBI	1990s-present	Constitutionally disputed	NSA intelligence laundered into criminal prosecutions. Origin hidden from judges, prosecutors, defendants.
ECHELON/Five Eyes	NSA+4 partners	1966-present	Unreviewed	Global interception of all communications. Legal circumvention: each country spies on other's citizens.
Pegasus (FBI tested)	FBI (Israeli tech)	2019-present	Equipment retained	World's most invasive commercial spyware. Tested for American phones. Considered for domestic criminal use.
FinSpy (vs. Americans)	Ethiopian govt.	2014 confirmed	No consequence	Foreign government spied on American citizen on U.S. soil with commercial malware. Court: immune.
Utah Data Center	NSA	2014-present	Active	$3B facility storing all intercepted data. Capacity: multiple yottabytes. Designed to hold America's communications.
Dual EC DRBG Backdoor	NSA	2006-present	Active (standard)	NSA deliberately weakened the global encryption standard used by banks, governments, and consumers worldwide.

WHAT THIS ALL MEANS — FOR EVERY PERSON READING THIS

You have now read the complete confirmed public record. Here is what it means in plain terms.

Your Communications

Every phone call you make, every email you send, every search you type, every website you visit, every message you send on any platform — all of it passes through infrastructure that has been, and in many cases continues to be, intercepted and stored by government agencies. This is not hypothetical. The infrastructure was confirmed by court proceedings and a federal appeals court ruling. Section 702 of FISA — the legal authority for PRISM — is still in effect.

Your Devices

The hardware you use may contain firmware-level implants undetectable by any consumer security tool. The NSA built implants for every major hard drive brand. The CIA built tools that turn smart TVs into microphones. These capabilities were confirmed to exist. Whether any specific device is compromised cannot be determined from the outside.

Your Legal Rights in Court

If you are ever a defendant in a criminal case, there is a confirmed, documented, institutionalized system for concealing the true origin of the evidence against you from your own lawyer and the judge. Parallel construction has been in daily use since the 1990s. You have no way of knowing whether it was used in your case. This is confirmed by senior law enforcement officials speaking on the record.

Your Political Activity

COINTELPRO was formally ended in 1971. Its methods — infiltration, surveillance of political organizations, monitoring of protest movements — were confirmed by FBI documents as recently as 2017. The names of the programs change. The underlying capability has never been dismantled.

The Weapons That Exist

The United States government built cyberweapons. It lost some of them. EternalBlue destroyed hundreds of thousands of computers worldwide after it escaped the NSA. Stuxnet spread beyond its intended target. The CIA lost 34 terabytes of its hacking arsenal. These weapons are now in the world. The NSA also deliberately weakened the global encryption standard protecting banking, government, and private communications — reducing security for everyone in order to maintain a backdoor for itself.

THE BOTTOM LINE

Eight decades. Confirmed by Congress. Confirmed by courts. Confirmed by government officials on the record. The surveillance never stopped between exposures — it continued. The reforms never caught up to the technology — they always lagged. The whistleblowers were punished — not the programs. The public was lied to — by named officials, on the record, under oath. This is what happened. The record is open. The documents are real. Verify every claim. Share what you learn. Silence is how this continues.

PRIMARY SOURCES — VERIFY EVERYTHING YOURSELF

Every claim in this document can be traced to one of the following primary sources. All are publicly available.

SOURCE	WHERE TO FIND IT
Church Committee Final Reports (1976)	intelligence.senate.gov — full text available online, 6 volumes
Rockefeller Commission Report (1975)	ford.utexas.edu/library — digitized full text
NSA Inspector General Report on Stellar Wind (2009)	washingtonpost.com — published June 2013 with Snowden materials
Senate MKUltra Hearings (1977)	intelligence.senate.gov — 95mkultra.pdf
Snowden NSA Document Archive	The Guardian, Washington Post, The Intercept — published 2013-2015
WikiLeaks Vault 7	wikileaks.org/vault7/ — all 8,761 documents
CIA WikiLeaks Task Force Report (2017)	CNN, June 16, 2020 — FOIA release
NSA ANT Catalog	Der Spiegel, December 29, 2013; EFF hosts full PDF
Reuters Parallel Construction Investigation	reuters.com, August 5, 2013 — 'U.S. Directs Agents to Cover Up Program'
AT&T Room 641A — Mark Klein Declaration	eff.org — filed in Hepting v. AT&T, 2006
FBI COINTELPRO Declassified Files	vault.fbi.gov/cointel-pro
ACLU Stingray FOIA Documents	aclu.org/issues/privacy-technology/surveillance-technologies

SOURCE	WHERE TO FIND IT
Utah Data Center Specifications	Army Corps of Engineers bid solicitation — publicly available
Kaspersky Equation Group Report (2015)	securelist.com — 'Equation Group: Questions and Answers'
European Parliament ECHELON Report (2001)	europarl.europa.eu — Final Report of the Temporary Committee on ECHELON
U.S. Court of Appeals — NSA Program Unlawful (2020)	United States v. Moalin, 9th Circuit, September 2, 2020
Senate Select Committee on Intelligence — NSA Oversight	intelligence.senate.gov
Privacy and Civil Liberties Oversight Board — XKeyscore (2021)	pclob.gov
IRS Parallel Construction Manual Entry	Reuters, August 7, 2013 — IRS Manual follow-up
New York Times — FBI and Pegasus (2022)	nytimes.com, January 28, 2022
National Security Archive — MKUltra Collection (2024)	nsarchive.gwu.edu — CIA and the Behavioral Sciences
Operation Olympic Games / Stuxnet	Washington Post and New York Times, June 1, 2012
Shadow Brokers / EternalBlue	Shadow Brokers release, April 14, 2017; WannaCry — Europol
FBI Carnivore FOIA Documents	archive.epic.org/privacy/carnivore/foia_documents.html

This document contains no classified information.

Every claim is sourced to publicly available government documents, court records, and authenticated whistleblower disclosures.

Verify independently. Share freely. The record is open.

Compiled April 2026 under independent research — Veritas Protocol